REMARKS

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached Appendix is captioned "**Version with Markings to Show Changes Made.**"

Claims 1, 2, 5, 6, 8, 16-19 stand rejected under 35 U.S.C. §102(b) as being anticipated by Blakely et al. (U.S. Patent No. 5,677,952). In response, Applicants amended claims 1, 8, 18 and 19 to more clearly define the features of the present invention, without narrowing their scope, and respectfully traverse. Applicants respectfully traverse because the cited reference does not disclose (or suggest) encrypting different key data for each unit storage area with a password, and writing (storing) each encrypted key data on the storage medium, as now recited in amended 1 and 8, and similarly recited in claims 18 and 19.

In one embodiment of the present invention, a plurality of different key data is generated for each sector of the disk. The encrypted key data for each sector is then computed by using a user password and the key data. The encrypted key data is then written to the storage medium. When writing to the storage medium, the write data is encrypted by the corresponding key data of the sector, and written to that sector of the disk. Similarly, when reading from the storage medium, the encrypted key data is read from the storage medium and the corresponding key data is decrypted by using the password. The read data from the sector is then decrypted by the corresponding key data to the plain text.

In contrast, the Blakely et al. reference discloses a data protecting method on a storage medium using pseudorandom values for each index of the storage medium. In the protecting method disclosed in Blakely et al., a secret key is derived from a password entered into the computer by the authorized user. The pseudorandom bit strings having a sector size length are generated from the secret key and sector index. The pseudorandom bit string is then used to encrypt and decrypt data accesses to and from the sector. However, the secret key is only maintained in the computer's volatile memory and is erased when the user logs off. (Col.2 lines 6-49).

Further, the secret key "a" is a bit string generated by the Secure Hash Algorithm, and is processed to convert it into a cipher fa. When the string x at position i of the disk is read, the value fa(i) is computed. A value y is computed by XORing x and fa(i), which replaces the previous value x for the sector. When y is read, fa(i) is computed, and the plain text x is decrypted by fa(i). The fa(i) is stored during log on, but again erased when the user is logged off (Col. 5, lines 1-9; Col. 5, line 40 to Col. 6, line 58).

Although the cited reference discloses the disk storing a corresponding table between changeable password and a secret key, the secret key a is derived from the user password by the hash algorithm and is stored only during log on. The pseudorandom bit string fa(i) is computed from the sector ID and the secret key a for each sector. When writing, the write data is encrypted by the corresponding string fa(i), and written to the sector of the disk. Similarly, when reading, the read data y from the sector is decrypted by the corresponding string fa(i) to the plain text x. Unlike the present invention, the fa(i) is stored during log on and erased when the user is logged off.

In addition, the cited reference discloses reading encrypted data from the storage medium, decoding the key with the password, and decrypting the data, but the decoded key is a secret key, and not the data encrypted by key data stored in each sector, as recited in the claims. As a result, the protecting method disclosed in Blakley et al. is applicable only to disk data fixed to a particular computer, because the secret key and the pseudorandom bit string are erased when log off occurs, to prevent access by unauthorized users when they log on. The protecting method of the present invention, on the other hand, can be used for both fixed disks and removable disks (medium and unit), because the encrypted key data for each sector are stored in the storage medium, and the stored and encrypted key data are read from the storage medium when read. In fact, it is preferred that the present invention protect data of removable disks (MO) or removable disk units (portable HDD).

However, the Blakley et al. reference does not disclose that different encrypted key data for each sector, which is computed by the different key data for each sector and the password, is written to the storage medium when writing and read from the storage medium to decrypt the key data. Blakley et al. do not disclose that the read data is then decrypted from the decrypted key data.

Claims 3, 4, 7, 9-14 and 15 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Blakely et al. In response, Applicants amended claim 15 to more clearly define the features of the present invention, without narrowing the scope of the claim, and respectfully traverse. Applicants respectfully traverse because the cited reference does not disclose or suggest "a plurality of key data encrypted with a different key data for each unit storage area of said storage medium with a password" and "a plurality of data encrypted with the key data corresponding to said unit storage area of said storage medium", as now recited in amended claim 15.

Applicants reassert the above argument asserted to overcome the §103 rejection of claims 1, 8, 18 and 19. Applicants further submit that since claims 3, 4, 7 and 9-14 depend upon claims 1 and 8, respectively, they necessarily include all of the features of the independent claim plus other additional features. Thus, Applicants submit that the § 103 rejection of claims 3, 4, 7 and 9-14 has also been overcome for the same reasons mentioned above to overcome the §103 rejection of independent claims 1 and 8. Applicants respectfully request that the §103(a) rejection of claims 3, 4, 7, 9-14 and 15 also be withdrawn.

For all of the above reasons, Applicants respectfully requestf reconsideration and allowance of all pending claims. The Examiner should contact the undersigned attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns
Registration No. 29,367

January 25, 2002
300 South Wacker Drive, Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Customer No. 24978
F:\DATA\WP60\3408\62676\AME-B.DOC

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

Claims 1, 8, 15, 18 and 19 were amended as follows:

1. (Twice Amended) A storage medium data protecting method of protecting data on a storage medium, comprising:

a step of generating key data, encrypting the key data with a password, and writing the encrypted key data to said storage medium;

a step of encrypting the data with the key data, and writing the encrypted data to said storage medium;

a step of reading the encrypted key data from said storage medium;

a step of decoding the encrypted key data with the password; and

a step of decoding the data on said storage medium with the decoded key data,

wherein said key data generating step comprises:

a step of generating different key data for each of a plurality of unit storage areas of said storage medium;

a step of encrypting each said different key data for each unit storage area with said password, and a step of writing each said encrypted key data to said storage medium,

and wherein said data encrypting step comprises a step of encrypting the data with the key data corresponding to said unit storage area to write the data,

and wherein said data decoding step comprises a step of decoding the data with the decoded key data corresponding to said unit storage area where the data have been read.

8. (Twice Amended) A storage medium data protecting apparatus for protecting data on a storage medium, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating key data, the key data with a password, writing the encrypted key data to said storage medium, encrypting the data with the key data, and writing the encrypted data to said storage medium;

a read mode of encoding, after reading the encrypted key data from said storage medium, the encrypted key data with the password, and decoding the data on said storage medium with the decoded key data, wherein [said key data comprises] said write mode comprises a mode of generating different key data for each unit storage area of said storage medium, encrypting each said different key data for each unit storage area with said password, writing each said encrypted key data to said storage medium, and encrypting the data with the key data corresponding to said unit storage area to write the data,

and wherein said read mode comprises a mode of decoding the data with the decoded key data corresponding to said unit storage area where the data have been read.

15. (Twice Amended) A storage medium having protected data is stored with;

a plurality of key data encrypted with a different password for each of a plurality of unit storage areas of said storage medium; and

a plurality of data encrypted with the [different] key data [for each] corresponding to said unit storage area of said storage medium.

18. (Once Amended) An encoding method protecting data on a storage medium, comprising:

a step of generating different key data for each unit storage area of said storage medium, encrypting the key data with a password, and writing the encrypted key data to said storage medium;

a step of encrypting the data with the key data corresponding to said unit storage area to which the data is to be written, and writing the encrypted data to said storage medium.

19. (Once Amended) A decoding of protected data on a storage medium, comprising:

a step of reading the encrypted key data which is encrypted with different key data for each unit storage area of said storage medium from said storage medium;

a step of decoding the encrypted key data with the password; and

a step of decoding the data on said storage medium with the decoded key data corresponding to said unit storage area where the data have been read.